AO 106 (Rev. 04/10) Application for a Search Warrant

UNITED STATES DISTRICT COURT

for the

District of New Mexico

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)

The residential property and premises at 812 Acapulco Road NE, Rio Rancho, NM 87144 (described in Attachment B, incorporated herein by reference)

Case No. 15-MR-636

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*

See Attachment B, incorporated herein by reference

located in the _____ District of New Mexico, there is now concealed *(identify the person or describe the property to be seized)*:

See attachment A, incorporated herein by reference

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 USC 2252	Distribution of any depiction involving the use of minors engaged in sexually explicit conduct.

The application is based on these facts:

See attached affidavit.

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Kelly Brammer
Applicant's signature

Kelly Brammer Special Agent
Printed name and title

Sworn to before me and signed in my presence.

Date: 10/14/15

Judge's signature

City and state: Albuquerque, NM

William P. Lynch, U.S. Magistrate Judge
Printed name and title

AFFIDAVIT
IN SUPPORT OF
APPLICATION FOR SEARCH WARRANT

Your Affiant, Kelly Brammer, having been first duly sworn, does hereby depose and state as follows:

Introduction

1. Your Affiant is a Special Agent of the Federal Bureau of Investigation (FBI). Your Affiant has been a Special Agent (SA) since August 2014. As such your Affiant is a "federal law enforcement officer" within the meaning of Federal Rule of Criminal Procedure 41(a)(2)(C), that is, a government agent engaged in enforcing the criminal laws and duly authorized by the Attorney General to request search warrants. Your Affiant is currently assigned to the FBI's Albuquerque Violent Crime Program, as such, your Affiant is authorized to investigate violations of federal child pornography and exploitation laws. The information set forth in this affidavit was derived from your Affiant's own investigation and/or communicated to your Affiant by other sworn law enforcement officers. SA Victoria Vaughan has drafted and executed multiple search warrants for alleged violations of laws relating to the sexual exploitation of minors and has contributed her knowledge and experience in the drafting of this affidavit. Because this affidavit is submitted for the limited purpose of securing a search warrant, your Affiant has not included each and every fact known to your Affiant concerning this investigation. Your Affiant has set forth only those facts that your Affiant believes are necessary to establish probable cause to support a search warrant for the residence at 812 Acapulco Road NE, Rio Rancho, NM 87144.

Relevant Statutes

2. This investigation concerns alleged violations of certain activities relating to material involving the sexual exploitation of minors: Title 18 U.S.C. 2252(a)(2). According to 18 U.S.C. 2252(a)(2), it is a federal crime for a person who "knowingly receives, or distributes, any visual depiction using any means or facility of interstate or foreign commerce, …, if-

(A) The visual depiction involves the use of a minor engaging in sexually explicit conduct; and

(B) Such visual depiction is of such conduct."

Computers and Child Pornography

3. Computers and computer technology have revolutionized the way in which individuals interested in visual depictions of minors engaged in sexually explicit conduct ("child pornography"), as defined in 18 U.S.C. § 2256, interact with each other. Trading child pornography on the Internet is open, anonymous, and engaged in worldwide.

4. Your Affiant knows that computer hardware consists of all equipment that can collect, analyze, create, display, convert, store, conceal or transmit electronic, magnetic, optical or similar computer impulses or data. Hardware includes any data processing devices such as central processing units, memory typewriters and self-contained "laptop" or "notebook" computers, IPads, IPods, Tablets, and Portable gaming devices, as well as internal storage devices such as fixed hard disks, floppy disk drives and diskettes, magnetic tape drives and tapes, optical storage devices, and other memory storage

devices, as further described in Attachment A, incorporated herein by reference. Some computer hardware can be internal to the computer system or external. The external component hardware is often referred to as peripheral and includes input/output devices such as keyboards, printers, scanners, plotters, video display monitors and optical readers, web cameras, communication devices such as modems, recording equipment, RAM or ROM units, automatic dialers, video/digital camera equipment, flash drives, thumb drives, key drives, USB devices, removable/portable hard drives, media cards (including xD-Picture cards, Multi Media cards, Compact Flash cards, Memory Sticks, Secure Digital Cards, Solid State drives), CDs, DVDs, Blu-ray discs, minidiscs, other optical disks, and other external media.

5. Your Affiant has learned from experienced agents that computer files or remnants of such files on computers and computer related media can be recovered months or even years after they have been downloaded, deleted, or viewed via the Internet. Electronic files downloaded to a hard drive can be stored for years at little to no cost. Even when such files have been deleted, they can be recovered months or years later using readily-available forensic tools. When a person "deletes" a file on a computer and/or computer related media, the data contained in the file does not actually disappear; rather, that data remains on the media until it is overwritten by new data. The actual file is not initially erased or removed from the computer and/or computer related media, but rather, it remains available in free space on the computer and/or computer related media until overwritten by other information. The "deleted" file can also be overwritten by information when the computer user takes a positive action to permanently remove the

"deleted" file from the hard drive, such as employing "wiping" software, formatting the hard drive, or de-fragmenting or compressing the information located on the hard drive. However, "deleted" files which have not yet been overwritten by other information can often be successfully recovered during the search of a computer system or computer related media. These "deleted" files are often recovered long after the date the criminal activity occurred. Similarly, files that have been viewed via the Internet are automatically downloaded into a temporary Internet directory or cache. The browser typically maintains a fixed amount of hard drive space devoted to these files, and the files are only overwritten as they are replaced with more recently viewed Internet pages.

6. Your Affiant knows that computers and computer related media's ability to store images in digital form makes them an ideal repository for child pornography. A single DVD, CD-ROM, jump drive, hard drive, thumb drive, compact flash, other memory cards and other devices (as referenced in Attachment A) can store thousands of images and hundreds of thousands of pages of text, with storage capacities increasing all of the time. The size of the fixed electronic storage media (commonly referred to as the hard drive) used in home computers has grown tremendously within the past several years. Hard drives with a capacity of one hundred gigabytes or more are not uncommon. These drives can store hundreds of thousands of images at a very high resolution. Electronic storage located in host computers adds another remote dimension to this storage equation.

7. Your Affiant knows that computer software is digital information, which can be interpreted by a computer and any of its related components to direct the way they work.

Software is stored in electronic, magnetic, optical or other digital form. It commonly includes programs to run operating systems, applications such as word processing, graphics or spreadsheet programs, utilities, compilers, interpreters and communications programs.

8. Your Affiant has learned from experienced agents that computer passwords and data security devices are designed to restrict access to, or hide, computer software, documentation or data. Data security devices may consist of hardware, software or other programming code. A password, a string of alpha-numeric and/or special characters, usually operates as a sort of digital key to "unlock" particular data security devices. Data security hardware may include encryption devices, chips and circuit boards. Data security software or digital codes may include programming code that creates "test" or "hot" keys that perform pre-set functions when depressed. "Hot" keys can be designed to erase, or otherwise render unusable, data that was contained within computer memory storage devices.

9. Your Affiant knows that documents can be created through the use of computer software programs, and that those documents can be used to facilitate the commission of crimes. In some cases, the mere possession of certain types of documents constitutes criminal conduct. Computer systems also can store information in internal or peripheral storage devices including fixed disks, floppy diskettes, tape drives, optical storage devices or other memory storage devices such as flash drives, thumb drives, key drives, USB devices, IPods, IPads, PSP Players, removable/portable hard drives, media cards

(including xD-Picture cards, Multi Media cards, Compact Flash cards, Memory Sticks, Secure Digital Cards, Solid State drives), CDs, DVDs, Blu-ray discs, minidiscs, other optical disks, and other external media. Based on my training and experience, and my personal use of computer systems in my employment as a Special Agent, I know that users of computer systems often save information or create documents and save them to various types of computer-related storage devices, both internally, such as the hard drive, and externally, such as a thumb drive.

10. Your Affiant knows that computers are expensive and that people tend to keep them in their possession over lengthy periods of time. Even after people buy a new computer they often do not dispose of their old computer. It is common for people to possess old computers for several years because they do not want to dispose of an item that was expensive, they want to access information on the old computer, or because they do not know how to delete the personal information they have accrued on their computer.

11. Your Affiant knows through training and experience that people who distribute child pornography often keep child pornography on portable media devices. The use of portable devices for child pornography makes it easier for users to conceal and access remotely.

12. Your Affiant knows from training and experience, and the training and experience of other law enforcement personnel with whom your Affiant has spoken, that those persons who trade, receive, or distribute, images of minors engaged in sexually explicit conduct

often view children as sexual objects, and that such persons often receive gratification from sexually explicit images of minors.

13. Your Affiant knows that persons who distribute, or receive images of child pornography are often found to distribute, receive, or possess material containing sexually explicit conduct involving multiple minor victims.

14. Your Affiant knows from training and experience that those persons who trade, receive, or distribute sexually explicit images of minors often maintain their sexually explicit images of minors, and that such images can include all types of media such as still photographs, digital photographs, video clips, digital video clips, printouts, magazines, and videotapes. From training and experience of other agents with whom your Affiant has spoken, many individuals interested in child pornography have admitted being addicted to the images and find sexual gratification in said images. Your Affiant knows that currently the most prevalent media used is digital media, including digital photographs and digital video clips that could be stored on the possessor's computer hard drive, computer diskettes, CD ROM's, and various external computer memory storage devices, such as flash drives, thumb drives, key drives, USB devices, IPods, IPads, tablets, PSP Players, gaming systems, removable/portable hard drives, media cards (including xD-Picture cards, Multi Media cards, Compact Flash cards, Memory Sticks, Secure Digital Cards, Solid State drives), CDs, DVDs, Blu-ray discs, minidiscs, other optical disks, and other external media, some of which can be extremely small and stored easily in personal safes, lockboxes, vehicles, or on one's person. Additionally, your

Affiant knows from training and experience, that digital images are easily printable in "hard copy" form and can be stored virtually anywhere inside a residence, vehicle, boat, garage, sheds, bank safety deposit boxes, lock boxes, and personally-owned safes, as well as other areas under the control of those persons possessing, distributing, and receiving sexually explicit images of minors.

15. Further, your Affiant knows that digital media storage devices including "thumb drives," "flash drives," "pen drives," or memory sticks are by their very nature designed to be small enough to carry in one's pocket or affixed to a key chain. Also, your Affiant is aware that digital cameras and video recording devices contain storage disks that are like "thumb drives," in that they can hold large quantities of data, and come in very small sizes. Your Affiant knows that such storage devices are able to store digital images, and by their nature are extremely portable and can easily be concealed on one's person or in one's clothing.

16. Your Affiant knows that many cellular telephones, "smart phones," and Personal Digital Assistants (PDA's) are capable of receiving, distributing and possessing child pornography images through infrared transmissions as a picture message or attachment to a text message sent to or received from other cellular telephones, PDA's, and computers. Many models of cellular telephones and PDA's have two storage capabilities. The device may have built-in memory capable of holding child pornography images/videos and also utilize removable storage options capable of holding child pornography images (such as but not limited to compact flash cards, secure digital cards, and memory sticks). Many of

these storage cards are capable of being read by computers, other cellular telephones, PDA's, other digital cameras and can be loaded directly onto printers.

17. Your Affiant knows through training and experience, and the training and experience of other law enforcement officers, that those persons who receive and distribute sexually explicit images involving minors oftentimes use digital media such as digital still cameras and digital video recorders to capture and upload such sexually explicit images, including photographing said images that appear on a computer screen. Your Affiant also knows through training and experience and the training and experience of other agents that standard 35mm cameras and film can be used to capture such sexually explicit images.

18. Your Affiant knows through training and experience that undeveloped 35mm film located within residences being searched for the presence of images depicting sexually explicit conduct by minors is considered evidentiary in nature. Your Affiant further knows that the seizure and processing, including the development, is essential in determining the presence of further evidence.

19. Your Affiant knows that those persons seeking to distribute sexually explicit images of minors most often use the Internet to do so. The Internet is a worldwide network that connects computers and allows communication and transfer of data, information, and images across state and national boundaries. Individuals who use the Internet can communicate electronically by using e-mail. E-mail messages can contain text, data, and images. This type of communication is private in that it is directed from one Internet user

to another. Internet users can also communicate using chat rooms and instant messaging. Both chat rooms and instant messaging incorporate "real time" communication between Internet users. Instant messaging, like e-mail, is private, in that it is one Internet user communicating specifically, and exclusively, with another. Internet Service Providers such as America Online (AOL), and web sites such as Yahoo! provide software and venue for such one to one contact. The Internet offers a number of facilities which allow users to access, distribute, and exchange information including the World Wide Web (WWW), File Transfer Protocol (FTP), electronic e-mail (E-mail), and postings on newsgroups. The WWW allows users to display and access data in a multimedia format. FTP is a method of distributing and receiving files between computer systems. A newsgroup is an Internet site that is devoted to a particular area of interest or discussion including child pornography. Users may send or post messages and responses to be read at any time by others, much like a bulletin board.

20. Evidence of distribution of child pornography is often found on the user's computer and other computer media. As is the case with most digital technology, communications by way of computer can be saved or stored on the computer and other media used in connection with child pornography. Storing this information can be intentional, i.e., by saving an e-mail as a file or saving the location of one's favorite websites for example, bookmarked files. Digital information can also be retained unintentionally, e.g., traces of the path of an electronic communication may be automatically stored in many places (e.g., temporary files or Internet Service Provider client software, among others). Additionally, computer user's Internet activities generally leave traces or footprints in the

web cache and history files of the browser used. A forensic examiner can often recover evidence of child pornography in this intentionally and unintentionally retained digital information.

21. Your Affiant knows through training and experience that digital evidence, including registry file and other data may exist on computers that can be used to prove the identity of those who use the computer and computer related media and their possible involvement with visual depictions of minors engaged in sexually explicit conduct.

22. As further described in Attachment A, this warrant seeks permission to search and seize certain records related to violation of 18 U.S.C. § 2252 that exist in the subject location in whatever form they are found. One form in which the records may be found is stored on a computer's hard drive or other electronic media. Some of these electronic records might take the form of files, documents, and other data that is user-generated. Some of these electronic records may be in a form that becomes meaningful only upon forensic analysis.

23. Although some of the records called for by this warrant might be found in the form of user-generated documents (such as word processor, picture and movie files), computer hard drives can contain other forms of electronic evidence that are not user-generated. In particular, a computer hard drive may contain records of how a computer has been used, the purposes for which it was used and who has used these records. For instance, based upon your Affiant's knowledge, training and experience, as well as information related to

me by agents and others involved in the forensic examination of digital devices, your Affiant knows:

a. Data on the hard drive not currently associated with any file can provide evidence of a file that was once on the hard drive but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file);

b. Virtual memory paging systems can leave traces of information on the hard drive that show what tasks and processes the computer were recently in use;

c. Web browsers, e-mail programs and chat programs store configuration information on the hard drive that can reveal information such as online nicknames and passwords;

d. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices and the times the computer was in use;

e. Computer file systems can record information about the dates files were created and the sequence in which they were created. This information may be evidence of a crime or indicate the existence and location of evidence in other locations on the hard drive.

24. Further, in finding evidence of how a computer has been used, the purposes for which it was used and who has used it, sometimes it is necessary to establish that a particular thing is not present on a hard drive or that a particular person (in the case of a multi-user computer) was not a user of the computer during the time(s) of the criminal activity. For

instance, based on your Affiant's knowledge, training and experience, as well as information related to me by agents and others involved in the forensic examination of digital devices, your Affiant knows that when a computer has more than one user, files can contain information indicating the dates and times that files were created as well as the sequence in which they were created, and, for example, by reviewing the Index.dat files (a system file that keeps track of historical activity conducted in the Internet Explorer application), whether a user accessed other information close in time to the file creation dates, times and sequences so as to establish user identity and exclude others from computer usage during times related to the criminal activity.

25. Evidence of how a digital device has been used, what it has been used for and who has used it, may be the absence of particular data on a digital device and requires analysis of the digital device as a whole to demonstrate the absence of particular data. Evidence of the absence of particular data on a digital device is not segregable from the digital device.

26. The types of evidence described above may be direct evidence of a crime, indirect evidence of a crime indicating the location of evidence or a space where evidence was once located, contextual evidence identifying a computer user and contextual evidence excluding a computer user. All of these types of evidence may indicate ownership, knowledge and intent.

27. This type of evidence is not "data" that can be segregated, that is, this type of data cannot be abstractly reviewed and filtered by a seizing or imaging agent and then transmitted to

investigators. Rather, evidence of this type is a conclusion, based on a review of all available facts and the application of knowledge about how a computer behaves and how computers are used. Therefore, contextual information necessary to understand the evidence described in Attachment A also falls within the scope of the warrant.

28. Based upon your Affiant's knowledge, training and experience, as well as information related your affiant by agents and others involved in the forensic examination of digital devices, your Affiant knows that it is necessary to seize all types of electronic devices capable of storing digital evidence as described in this Affidavit and Attachment A for off-site review because computer searches involve highly technical, complex and dynamic processes.

29. Your Affiant knows through training and experience that individuals that show an interest in visual depictions of minors engaged in sexually explicit conduct may have in their possession journals correspondence and other writings detailing their and others involvement with visual depictions of minors engaged in sexually explicit conduct or a sexual interest in children. Your Affiant knows that these individuals may also keep records related to their internet service provider and internet services.

Child Pornography and Peer To Peer File Sharing

30. Your Affiant knows the following about individuals who distribute child pornography:

31. Many individuals who distribute child pornography are persons who have a sexual attraction to children. They receive sexual gratification and satisfaction from sexual fantasies fueled by depictions of children that are sexual in nature.

32. Many individuals who distribute child pornography possess sexually explicit materials, including photographs, magazines, digital videos, video tapes, books, slides, computer graphics or other images for their own sexual gratification. The majority of these individuals also possess child erotica, which may consist of images or text that do not rise to the level of child pornography but nonetheless fuel their deviant sexual fantasies involving children.

33. Many individuals who distribute child pornography often seek out like-minded individuals, either in person or on the Internet, to share information and trade depictions of child pornography and child erotica as a means of gaining status, trust, acceptance, and support. This contact helps these individuals to rationalize and validate their deviant sexual interest and associated behavior. The different Internet-based vehicles used by such individuals to communicate with each other include, but are not limited to Peer to Peer file sharing, e-mail, e-mail groups, bulletin boards, Internet Relay Chat, newsgroups, social networking sites, instant messaging, and other similar devices.

34. Many individuals who distribute child pornography maintain books, magazines, newspapers, and other writings, in hard copy or digital medium, on the subject of sexual activities with children, as a way of understanding their own feelings toward children,

justifying those feelings and finding comfort for their illicit behavior and desires. Such individuals rarely destroy these materials because of the psychological support they provide.

35. Many individuals who distribute child pornography maintain copies of names, addresses (including email addresses), phone numbers, or lists of persons who have advertised or otherwise made known in publications and on the Internet that they have similar sexual interests. These contacts are maintained as a means of personal referral, exchange or commercial profit. These names may be maintained in the original medium from which they were derived, in telephone books or notebooks, on computer storage devices, or merely on scraps of paper.

36. Your Affiant knows the following about Peer-to-Peer File Sharing:

37. The Internet is a worldwide network of computer systems operated by governmental entities, corporations, and universities. In order to access the Internet, an individual computer user must subscribe to an access provider, which operates a host computer system with direct access to the Internet. The access provider will then assign an Internet Protocol (IP) address to a subscriber. The World Wide Web (www) is a functionality of the Internet, which allows users of the Internet to share information.

38. A growing phenomenon on the Internet is Peer-To-Peer (P2P) file sharing. P2P file sharing programs are a standard way to transfer files from one computer system to

another while connected to a network, usually the Internet. P2P file sharing programs allow groups of computers using the same file sharing network and protocols to connect directly to each other to share files. While there are several P2P networks currently in operation, one predominant network is Ares. Individuals who distribute child pornography often use a P2P file sharing program like Ares.

Specifics of Search and Seizure of Computer Systems

39. Searches and seizures of evidence from computers require agents to seize all computers, and their components, and all computer items (computer hardware to include the computer and external storage devices, computer software, and computer related documentation as described in Attachment A) to be processed later by a qualified computer expert in a laboratory or other controlled environment. This is true because of the following:

a. Computer storage devices (like hard disks, diskettes, tapes, laser disks, magneto opticals, thumb drives and others) can store the equivalent of thousands of pages of information. Especially when the user wants to conceal criminal evidence, he or she often stores it in random order and with deceptive file names. This requires searching authorities to examine all the stored data to determine whether any of the evidence to be seized as set forth in this search warrant is contained in the stored data. This sorting process can take days or weeks, depending on the volume of data stored, and it would be generally impossible, due to the equipment needed and the time necessary, to accomplish this kind of data search on site;

b. Searching computer systems for criminal evidence is a highly technical process requiring expert skill and a properly controlled environment. The vast array of computer hardware and software available requires even computer experts to specialize in some systems and applications, so it is difficult to know before a search which expert should analyze the system and its data. The search of a computer system is an exacting scientific procedure which is designed to protect the integrity of the evidence and to recover hidden, erased, compressed, password protected, or encrypted files. Since computer evidence is extremely vulnerable to tampering or destruction (which may be caused by malicious code or normal activities of an operating system), the controlled environment of a laboratory is essential to its complete and accurate analysis. It is also important to obtain passwords to review information that may be hidden or have restrictive access.

Details of the Investigation

40. Your Affiant has viewed all videos described in this affidavit.

41. On March 25, 2015, SA Jay Ratliff of the New Mexico Internet Crimes Against Children Task Force (Task Force) conducted an investigation on the Ares P2P file sharing network. SA Ratliff identified a computer utilizing the IP address of 67.0.246.190. Investigators located the computer by conducting keyword searches for files related to child abuse, including child pornography on the Ares network.

42. On March 25, 2015, the Ares client P2P program on the computer with the IP address 67.0.246.190 reported its Ares nickname as: anon_4300f6be@Ares.

43. On March 25, 2015, between 12:15 hours and 13:44 hours Mountain Standard Time (MST), SA Ratliff successfully completed a single-source download of a file that the computer at IP address 67.0.246.190 was making available. The file is titled "(pthc) scargirl-compilation (2).avi" and is 13:55 in length. The video showed a young girl wearing blue jeans, a red-tshirt, and glasses masturbating an adult male and then performing oral sex on him. A young girl is then seen masturbating herself in the shower and the video then cuts to a different clip of a girl masturbating herself on a bed. The camera zooms in on her vagina and anus multiple times. There is also footage of a girl performing oral sex on an adult male. Your Affiant believes the girls to be between 7 and 10 based on no breast development and body size comparison. The last footage is of a girl masturbating an adult male, your Affiant believes the girl to be between the ages of 6-8 years old based on no breast development and body size comparison.

44. On March 25, 2015, between 19:52 hours and 20:22 hours MST, SA Ratliff successfully completed a single-source download of a file that the computer at IP address 67.0.246.190 was making available. The video is titled "(pthc pthc) stickam 2009 julie 3 ten year olds," and the length of the movie is 17.25. The video depicts three girls, who your Affiant believes to be between the ages of 8 to 12 years old based on no breast development and slight pubic hair. Using a webcam, the girls expose their breasts, buttocks, and vagina. One of the girls, wearing a gray T-shirt, lifts up her leg, exposing her vaginal lips and her anus.

45. On March 25, 2015, between 21:29 hours and 22:01 hours MST, SA Ratliff successfully completed a single-source download of a file that the computer at IP address

67.0.246.190 was making available. The video has no title, but is identified by hash value XXXXXX57GK and is 34 minutes in length. A girl with a red shirt and headband sits in front of a webcam. Your Affiant believes the girl to be between the ages of 10-12 based on no pubic hair and body size. The girl sits on a desk and exposes her vagina. She then inserts a green object resembling a pen into her vagina, and subsequently touches herself with the object.

46. On March 25, 2015, between 1517 hours and 1600 hours MST, SA Ratliff successfully completed a single-source download of a file that the computer at IP address 67.0.246.190 was making available. The video is titled "pthc!!-new!! S (compilation)-Yes" and is 3:16 in length. The video depicts three girls who your Affiant believes to be between the ages of 10-13 based on slight pubic hair and breast development. They are first seen clothed and holding a sign that says "Welcome to Dark Seductresses. We'll Make Your Dick Stay Rock Hard." The girls act out a burglary scene where two girls are forced to take off their clothes and up close shots of their vaginas and anus are seen.

47. On April 14, 2015, SA Ratliff obtained a Grand Jury Subpoena Duces Tecum from the 2nd Judicial District for CenturyLink and for IP address 67.0.246.190.

48. On April 26, 2015, CenturyLink responded with the following subscriber information for 67.0.246.190:

> Valentin E. Vigil
> 812 Acapulco Road
> Rio Rancho, NM 87144
> Associated phone number: 505-892-5291
> Telephone number – 505-552-7511
> Last payment transaction: 03/19/2015, with sugar577@msn.com, with card account ending in 0777.

49. On May 5, 2015, SA Ratliff provided the Subpoena and his report to SA Victoria Vaughan of the FBI.

50. From July 15-18, 2015, New Mexico Attorney General's Office (NMAGO) SA Owen Pena completed single-source downloads of multiple files that a computer utilizing IP address 97.123.21.177 and Ares nickname anon_617b15b1@Ares, was making available.

51. On July 15, 2015, between 12:54 hours and 13:13 hours MST, SA Pena successfully completed a single-source download of a file that the computer at IP address 97.123.21.177 was making available. The download is titled "lsmagazine lsm muuuuuuuitogostosinha.mpg" and the length of the movie is 7:22. The video shows a young girl who your Affiant believes to be between the ages of 10-12 based on slight breast development and slight pubic hair. She is nude, except for a small lime green shirt, cut above her breasts, exposing her breasts. She is wearing white boots with heels. The video starts with a close up shot of her vagina and anus. She begins dancing swaying her hips to the right and left, while smiling at the camera. She uses the chair as a prop, puts her leg on top of the chair, exposing her vagina to the camera. There are several close up views of her vagina.

52. On July 17, 2015, between 13:21 hours and 15:17 hours MST, SA Pena successfully completed a single-source download of three (3) files that the computer at IP address 97.123.21.177 was making available. The first video is titled "(sdpa) pthc loli lebina chair bondage & dad (2).wmv" and is 6:00 minutes in length. When the video begins playing, a title to the video appears stating "One month after defloration. Part 2. Tie-up and in-out game. Lelik." The video begins with a nude young girl who your Affiant believes to be

12-13 years old based on slight breast development and pubic hair. She and an adult male wearing a dark shirt, move a table. The girl kneels in front of a chair and lays her chest down on the chair. The man then uses rope to tie her wrists to the outside of the chair and tie her knees to the bottom part of the chair. The man takes off his pants and underwear and kneels behind the girl. His penis is erect and begins penetrating her vagina from behind her.

53. The second video is titled "(pthc) webcam_13yr pretty polish girl striptease" and is 15:53 in length. The video is a webcam video and shows a young girl wearing a red shirt, necklace, and jeans. She takes off her shirt and bra. Your Affiant believes her to be between the ages of 13-15, based on breast development. She then takes off her pants and underwear; there is no visible pubic hair. The camera zooms in on an up close shot of her vagina and anus.

54. The third video is titled "(spda) pthc new loli lebina fucked by dad" and is 6:23 in length. It appears to be a video of the same girl and man in the video described in paragraph 52: "(sdpa) pthc loli lebina chair bondage & dad (2).wmv." As the video begins to play, the following title appears "One month after defloration. Part 3. In-out." The video begins with a nude young girl who your Affiant believes to be 12-13 years old based on slight breast development and pubic hair. The girl is seen sitting in the same chair featured in the previous video. The man is kneeling in front of her and begins to penetrate her vagina with his penis. She is covering her face with her hands. At one point in the video, she attempts to push him off, but he continues penetrating her.

55. On July 18, 2015, between 13:47 hours and 13:55 hours MST, SA Pena successfully completed a single-source download of a file that the computer at IP address 97.123.21.177 was making available. The video is titled "!!new (pthc) cindy (private) (3)" and is 0:40 in length. This video begins by showing a young girl's pelvic area. She pulls down her underpants and is wearing a pink shirt. Your Affiant believes her to be between the ages of 5-7 based on a lack of pubic hair and no breast development and body size. A person's hand is seen touching her vagina, and then the person appears to kiss or insert their tongue in the young girl's vagina. The person then turns her around and squeezes her buttocks.

56. On July 24, 2015, Pena provided a report, grand jury subpoena results, and evidence to the FBI. The subpoena was served on the provider of IP address 97.123.21.177, which was Century Link. Their response indicates the above IP address was utilized from 07/15/2015-07/18/2015 to the following subscriber:

Valentin Vigil
812 Acapulco Road
Rio Rancho, NM 87144
Account number: 505 892 5291 551
Last payment transaction: 04/24/2015, with sugars577@msn.com, with card account ending in 0777.

57. From July 23-August 1, 2015 NMAGO SA Ratliff completed a single-source download of multiple files that a computer utilizing IP address 97.123.18.90 and Ares nickname anon_617b125a@Ares, was making available.

58. On July 23, 2015 between the hours of 1938 and 2042 MST, SA Ratliff successfully completed a single-source download of a file that the computer at IP address

97.123.18.90 was making available. The video is titled "!new!(pthc) laura strip dance (2)" and is 5:31 in length. The hash value is XXXXXATZD. The video shows a girl clothed in light pants and light shirt. She is laying on a bed with a blue and white plaid comforter. She begins taking off her blue and white striped socks. She takes her clothes off and dances around the room. She has no pubic hair and slight breast development, and appears to be between the ages of 8-12. There are up close shots of her vagina and her touching her vagina.

59. A search of the NMEC database of hash value XXXXXATZD indicates that the above video is an identified child.

60. On July 25th, between 005 hours and 0031 hours MST, SA Ratliff successfully completed a single-source download of a file that computer at IP address 97.123.18.90 was making available. The video is titled "new ptsc pthc spycam voyeur (24)." The video is 0:30 in length. A girl is sitting in bed/seat and an adult is helping her put pink colored pants on. The camera zooms in and focuses on the girl's vagina before she puts her pants on. Your affiant believes the girl to be between the ages of 4-7 based on no breast or pubic hair development.

61. On August 1, 2015, between the hours of 1202 and 1223 MST, SA Ratliff successfully completed a single-source download of a file that computer at IP address 97.123.18.90 was making available. The video is titled "!!!new!!!stpetersburg (girl12) 02(2)." The video is 1:19 in length. The video is of a nude girl, who your affiant believes is between the ages of 10 and 12 years based on slight breast and pubic hair development. She is

standing in a room, she then sits down, spreads her legs, and the camera zooms in to display up close views of her vagina.

62. On August 27th, 2015, FBI SA Brammer served a subpoena on the provider of IP address 97.123.18.90, which was Century Link. Their response indicates the above IP address was utilized from 07/23/2015-08/1/2015 to the following subscriber:

Valentin E. Vigil
812 Acapulco Road
Rio Rancho, NM 87144
Account number: 505 892 5291 551
Last payment transaction: 08/26/2015, with sugars577@msn.com, with card account ending in 0777.

63. On July 21, 2015, SA Vaughan conducted surveillance on 812 Acapulco Road, Rio Rancho, NM 87144 and observed a tan Nissan sedan, New Mexico plate 479 RMZ. The vehicle is registered to Gilbert Vigil or Clara Vigil, 812 Acapulco Road NE, Rio Rancho, NM 87144. On August 5, 2015, SA Paul Wright conducted surveillance on 812 Acapulco Road, Rio Rancho, NM 87144 and observed a silver Toyota Camry sedan, New Mexico plate 614 SJK. The vehicle is registered to Holly Stewart, DOB October 29, 1996, 2111 Forest Trail SE, Rio Rancho, NM 87124. On October 7, 2015, SA Kelly Brammer conducted surveillance on 812 Acapulco Road, Rio Rancho, NM 87144 and observed the Nissan sedan, New Mexico plate 479 RMZ described above.

64. Records checks conducted on May 21, 2015 and September 29, 2015 indicate Valentin E. Vigil currently does not reside at 812 Acapulco Road, Rio Rancho, NM 87144. Vigil's wage information, vehicle registration, and open source database checks indicate Valentin and his wife live at 2475 Pecos Road, Chandler, Arizona 85224.

Interstate Nexus

65. Your Affiant believes that the element of "in or affecting interstate or foreign commerce" is satisfied for a violation of 18 U.S.C. §§ 2252(a)(2) and for the limited purpose of securing a search warrant.

66. Individuals who utilize P2P file sharing client programs, such as Ares, must connect to the Internet to share files with other individuals. In order to access the Internet and P2P file-sharing programs, an individual computer user must subscribe to an access provider, which operates a host computer system with direct access to the Internet. Your Affiant believes that the element of "in or affecting interstate or foreign commerce" is satisfied for a violation of 18 U.S.C. 2252 and for the limited purpose of securing a search warrant.

67. Based on all of the foregoing information there is probable cause to believe that evidence and instrumentalities of violations of Title 18 U.S.C. Section 2252, are located on the residential property and in the premises of 812 Acapulco Road NE, Rio Rancho, NM 87144. In consideration of the foregoing, your Affiant respectfully requests that this Court issue a search warrant for the residential property and premises known as at 812 Acapulco Road NE, Rio Rancho New Mexico 87144, as described in Attachment B, authorizing the search of the aforementioned premises, any outbuildings, vehicles, safes, locked boxes, and all persons present, for the items described in Attachment A, and the seizure of such items for the purpose of searching and analyzing them in a controlled environment.

I swear that this information is true to the best of my knowledge and belief.

Respectfully submitted,

Kelly Brammer
Special Agent
Federal Bureau of Investigation

Subscribed and sworn to before me this 14th day October, 2015

The Honorable _____
United State Magistrate Judge

ATTACHMENT A
LIST OF ITEMS TO BE SEARCHED AND SEIZED

All visual depictions, including still images, videos, films or other recordings, made by electronic or mechanical means that show a person under the age of 18 years engaged in sexual conduct or the lewd exhibition of the genitals, as defined in Title 18, United States Code, Section 2256 (hereafter child pornography), and any mechanism used for the possession or storage of the same in violation of 18 U.S.C. Section 2252, including:

a. Any computer, computer system and related peripherals including data processing devices and software (including central processing units; internal and peripheral storage devices such as fixed disks, external hard drives, floppy disk drives and diskettes, routers, computer compact disks, CD-ROMS, DVD, and other digital media storage devices); gaming systems, peripheral input/output devices (including keyboards, printers, video display monitors, scanners, digital cameras, PDAs, MP3 players, cellular telephones and any device capable of storing digital media to also include televisions capable of reading such digital media, jewelry or other objects determined to contain digital and related communications devices such as USB connectors or other connectors capable of connecting the device to a computer or other device), as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (including physical keys locks, and safes);

b. All materials or items which are sexually arousing to individuals who are interested in minors, but which are not in and of themselves obscene or which do not necessarily depict minors involved in sexually explicit conduct. Such material includes written

materials dealing with child development, sex education, child pornography, sexual abuse of children, incest, child prostitution, missing children, investigative techniques of child exploitation, sexual disorders, pedophilia, nudist publications, diaries, journals, and fantasy writings;

c. All books, magazines, documents, advertisements portraying children under the age of 18 years engaged in sexual conduct, posed in sexually explicit positions or that contains clothed or partially clothes children under the age of 18, commonly referred to as "child erotica";

d. All computer passwords and other data security devices designed to restrict access to or hide computer software, documentation, or data. Data security devices may consist of hardware, software, or other programming code;

e. All diaries, logs, notations, telephone/address books, telephone answering machine tapes, correspondence, e-mail, chat conversation and/or any other documentation tending to show any communication or correspondence with any companies or person supplying, distributing or trading in child sexual abuse materials, or sexual conduct with minors;

f. All documents including email to or from the occupants of the residence or documents relating to online services accounts to include bills, receipts, cancelled checks, bank statements, and applications;

g. All financial records, telephone records, correspondence, ledgers or other documents showing the purchase and/or sale of images of child sexual abuse material;

h. Documents and records regarding the ownership and/or possession of the searched premises, including person identification, bills, receipts, mail, utility bills, rental agreements, and bank statements;

i. All records related to internet usage;

j. All electronic equipment, projectors, televisions, VCRs and/or any other device, that will be needed to watch, playback or duplicate an item that was seized;

k. All locked boxes, safes, or containers;

l. During the course of the search, photographs of the searched premises may also be taken to record the condition thereof and/or the location of items therein;

m. Any computer hard drive or other electronic media found to contain information called for by this warrant to include the following:

   i. Evidence of who used, owned, or controlled the computer at the time the contraband described in this warrant were created, edited or deleted such as logs, registry information, saved usernames and passwords, documents and browsing history

   ii. Evidence of software used that would allow users to control the computer such as viruses, Trojan horses or other forms of malicious software

   iii. Evidence of attachment of other peripheral devices to the computer such as disks, thumb drives, external hard drives and other similar media

   iv. Bookmarks, internet history, temporary internet files, lnk files, cache files, and other items showing how the computer was accessed, who accessed the computer, and/or how the computer was utilized

   v. Metadata contained in an image or digital video

ATTACHMENT B
DESCRIPTION OF LOCATION TO BE SEARCHED

The residential property and premises of 812 Acapulco Road, Rio Rancho, New Mexico 87144, including all vehicles associated with occupants, outbuildings and persons present. 812 Acapulco Road, Rio Rancho, New Mexico 87144, is identified as follows:

812 Acapulco Road, Rio Rancho, New Mexico 87144 is a stucco two-story house with a Spanish tile roof and two-car garage. The numbers "812" are visible next to the garage. A picture of 812 Acapulco Road, Rio Rancho, New Mexico 87144 is attached.

812 Acapulco Road NE, Rio Rancho, NM 87144